SOLUTION BRIEF

FortiCWP Accelerates Threat Detection and Response

Executive Summary

With migration of applications to Infrastructure-as-a-Service (IaaS) and the increasing risk of security threats in the public cloud, organizations cannot easily detect and respond to threats fast enough in their hybrid and multi-cloud environments. FortiCWP provides centralized security monitoring and threat detection, enhanced by global, up-to-the-minute threat intelligence on botnets, zero-day exploits, and more. The result is faster detection and response and improved efficiencies for overstretched security teams.

Multi-cloud Environments Drive Gains, but Obscure Risks

Organizations have embraced the public cloud to a point where these services are expected to grow by another 23.1% in 2021 to $332.3 billion worldwide.[1] The benefits of the cloud are indeed compelling; they include increased flexibility, faster time to value, the ability to scale up or down as needed, and cost-efficiency from being able to pay only for resources used.

However, after a decade or more of aggressively adding cloud resources, security teams are struggling with cloud sprawl. Resources from different clouds have been added across multiple regions, all without centralized control. This makes it difficult to distinguish between legitimate activities and those that are illegitimate.

FortiCWP Enables Multi-cloud Threat Detection and Response

- Centralized visibility into threats
- Consistent security management across multi-cloud environments
- Predefined and custom threat-detection policies
- Automated threat-response workflows
- Real-time intelligence on advanced threats

The Fortinet FortiCWP Cloud Security Posture Management and Workload Protection solution offers comprehensive threat policies that come with predefined rules as well as the ability to customize threat policies. Further, leveraging extensive threat intelligence from years of research by FortiGuard Labs, FortiCWP offers predefined threat policies to address the most common misconfigurations and activity-related threats.

Figure 1: FortiCWP dashboard.

FortiCWP allows administrators to configure custom threat policies that correspond to an organization's needs. The threat policies can be defined based on severity, focused on content and activity events. Notifications can be configured, and for certain policies, remediation actions can be automated.

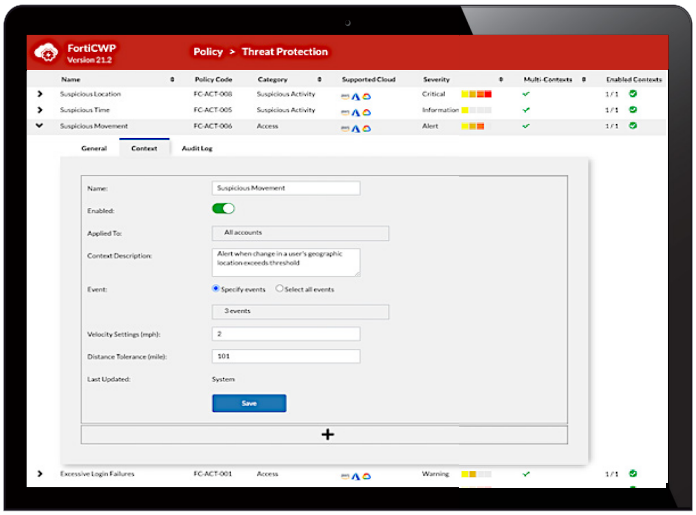

Figure 2: Predefined policies targeting the most common misconfigurations are available in FortiCWP.

To truly detect complex threats in public cloud environments, centralized visibility with comprehensive behavior and configuration-based policies are necessary. Threat intelligence also needs to be leveraged in real time for threat detection and prevention, regardless of which cloud the threat targeted. In cloud environments, suspicious activity and compromised accounts need to be blocked throughout. Threat intelligence powered by advanced artificial intelligence (AI) and machine learning (ML) methodologies, such as indicators of compromise (IOCs) from FortiGuard Labs, helps identify and prevent the propagation of new threats.

Centralized Multi-cloud Threat Visibility and Response

FortiCWP mitigates these challenges by providing:

- **Continuous and centralized security monitoring** of security elements such as configurations, user activity, traffic flow logs, and data storage in public cloud environments.
- **Out-of-the-box, predefined threat policies** that identify potential threats such as malicious traffic, suspicious user activity, and vulnerable configurations.
- **Custom policies** that are leveraged to best suit the unique organization's needs. FortiCWP delivers policies that are customizable based on relevant organizational needs, risk tolerance, and potential threats an organization is facing.
- **Faster investigations** due to alerts and detailed data analysis with full contextual details that shorten time to resolution.

Leveraging Global Threat Intelligence

FortiCWP receives live updates from FortiGuard Labs, the Fortinet global threat intelligence and research organization. In addition to the global threat hunting and analysis team, FortiGuard Labs also receives threat-intelligence feeds from over 200 partners. AI and ML enable researchers to better understand, classify, and protect Fortinet customers from malware and attacks, resulting in faster, more effective responses. This service ingests and analyzes over 100 billion security events from over 4.4 million sensors deployed globally, and produces approximately 1 billion security updates every day to Fortinet customers around the world. This enables customers to stay protected against new, unknown threats across all Security Fabric deployments.[2]

The network combines original research from strategic global security agencies, key technology partners, and cybersecurity alliances. All this information is fed back into FortiCWP, providing up-to-the-minute protection from zero-day threats, botnets, viruses, and other malicious exploits.

FortiGuard Labs databases used by FortiCWP include:

- **Zero-day exploits.** Over 900 zero-day exploits have been identified and profiled by FortiGuard Labs researchers to date.
- **IOCs.** FortiCWP also monitors for IOCs extracted from analyzing half a million malware samples on a daily basis. ML techniques capture malicious IP addresses, domains, and URLs.
- **Botnet IP data.** FortiGuard Labs uses aggregated botnet data to block 19 million botnet command-and-control attempts every minute of every day.
- **DevOps exploit data.** FortiCWP identifies suspicious DevOps activity or possible compromised accounts and alerts DevOps and security teams via email or notifications generated by services such as AWS Simple Queue Service (SQS) and Amazon Simple Notification Service (SNS).

Spotlight Threats in the Cloud

FortiCWP safeguards the business advantages of a multi-cloud environment by addressing threats effectively and quickly via centralized visibility, insight, and threat protection. To recap, FortiCWP provides critical protection advantages, including:

- Monitoring of ongoing cloud operations, configuration changes, and overall activity
- Correlation of data to identify nefarious and dangerous activity
- Predefined threat-prevention and threat-detection policies to address common cloud threats
- Customized threat-prevention policies
- Faster investigation of threats and suspicious activity

[1] "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021," Gartner, April 21, 2021.

[2] "FortiGuard Labs Consulting," Fortinet, December 3, 2020.

November 13, 2021 5:00 AM
377322-A-0-EN